Monitoring HX Storage Clusters

Monitoring HyperFlex Clusters

This chapter describes the monitoring content available through the following HX Storage Cluster interfaces:

- Cisco HX Connect

- Cisco HX Data Platform Plug-in

- Storage Controller VM command line

License Compliance and Feature Functionality

Beginning with Cisco HXDP Release 5.0(2a), full feature functionality and configuration changes require a valid Cisco HyperFlex Software License. HX Connect users with expired or insufficient licenses at the end of the evaluation or the grace period after the license compliance date, view a prominent countdown banner that alerts the user to the license compliance need and provides a link to the license renewal page until the license expiration is remedied.

In the event a license passes both the license expiration date and the grace period countdown, the current configurations will operate as expected with limited information. Renewing the license allows a user to resume full feature functionality, and make configuration changes. For details and examples of the banners, see the License Compliance and Feature Functionality section of the Cisco HyperFlex Systems Ordering and Licensing Guide.

To review the Cisco End User Agreement (Cisco EULA), see https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html

Monitoring HyperFlex Clusters with HX Connect

The Cisco HX Connect user interface provides a view of the Cisco HX storage cluster status, components, and features, such as encryption and replication.

Key monitoring pages include information about the local Cisco HX storage cluster:

- **Dashboard**—Overall Cisco HX storage cluster status.

- **Alarms, Events, Activity**—See the Cisco HyperFlex Systems Troubleshooting Reference Guide for details.

- **Performance**—Charts for IOPS, throughput, latency, and replication network bandwidth.

- **System Information**—HX storage cluster system-related information, including node and disk information, and access the HXDP Maintenance Mode.

  See the Cisco HyperFlex Systems Troubleshooting Reference Guide for generating support bundles, Storage Cluster Maintenance Operations Overview for entering and exiting maintenance mode, and Setting a Beacon to set a node or disk beacon.

- **Datastores**—Status and tasks related to datastores.

- **Virtual Machines**—Status and tasks related to protecting virtual machines.

Additional Cisco HX Connect pages provide management access:

- **Encryption**—For data at rest disk and node encryption tasks.

- **Replication**—For disaster recovery VM protection tasks.

The **Upgrade** page provides access to HX Data Platform and Cisco UCS Manager firmware upgrade tasks.

Dashboard Page

☞

Important If you are a read-only user, you may not see all of the options available in the Help. To perform most actions in HyperFlex (HX) Connect, you must have administrative privileges.

Displays a status summary of your HX storage cluster. This is the first page that you see when you log into Cisco HyperFlex Connect.

UI Element	Essential Information
Operational Status section	Provides the functional status of the HX storage cluster and application performance. Click **Information** (ⓘ) to access the HX storage cluster name and status data.

UI Element	Essential Information
Cluster License Status section	Displays the following link when you log into the HX storage cluster for the first time or till the HX storage cluster license is registered:
	Cluster License not registered link—Appears when the HX storage cluster is not registered. To register a cluster license, click this link and provide product instance registration token in the **Smart Software Licensing Product Registration** screen. For more information on how to get a product instance registration token, refer the **Registering a Cluster with Smart Licensing** section in the Cisco HyperFlex Systems Installation Guide for VMware ESXi.
	Beginning with HXDP Release 5.0(2a), HX Connect users with expired or insufficient licenses will be unable to access certain features or have limited feature functionality, for more information see License Compliance and Feature Functionality .
Resiliency Health section	Provides the data health status and ability of the HX storage cluster to tolerate failures.
	Click **Information** (ⓘ) to access the resiliency status, and replication and failure data.
Capacity section	Displays a breakdown of the total storage versus how much storage is used or free.
	Also displays the storage optimization, compression-savings, and deduplication percentages based on the data stored in the cluster.
Nodes section	Displays the number of nodes in the HX storage cluster, and the division of converged versus compute nodes. Hovering over a node icon displays that node's name, IP address, node type, and an interactive display of disks with access to capacity, usage, serial number, and disk type data.
VMs section	Displays the total number of VMs in the cluster as well as the breakdown of VMs by status (Powered on/off, Suspended, VMs with Snapshots and VMs with Snapshot Schedules).
Performance section	Displays an HX storage cluster performance snapshot for a configurable amount of time, showing IOPS, throughput, and latency data.
	For full details, see **Performance Page**.
Cluster Time field	System date and time for the cluster.

Table Header Common Fields

Several tables in HX Connect provide one or more of the following three fields that affect the content displayed in the table.

UI Element	Essential Information
Refresh field and icon	The table automatically refreshes for dynamic updates to the HX Cluster. The timestamp indicates the last time the table was refreshed. Click the circular icon to refresh the content now.
Filter field	Display in the table only list items that match the entered filter text. The items listed in the **current** page of the table below are automatically filtered. Nested tables are not filtered. Type in the selection text in the **Filter** field. To empty the **Filter** field, click the **x**. To export content from other pages in the table, scroll to the bottom, click through the page numbers, and apply the filter.
Export menu	Save a copy of the **current** page of table data. The table content is downloaded to the local machine in the selected file type. If the listed items are filtered, the filtered subset list is exported. Click the down arrow to select an export file type. The file type options are: `cvs`, `xls`, and `doc`. To export content from other pages in the table, scroll to the bottom, click through the page numbers, and apply the export.

Activity Page

Displays a list of recent activity on the HX storage cluster allowing you to monitor the progress of VM operations, Cluster upgrade/expansion, enter/exit maintenance mode, and recovery jobs.

UI Element	Essential Information

Activity list	Displays a list of recent tasks including the following details:
	
	• ID
	
	• Description
	
	• VM power on/off/suspend status
	
	• Task status:
	
	   • **In Progress**
	
	   • **Success**
	
	   • **Failed**
	
	    For failed VM-power operations, the **Existing State** and **Required State** fields are also included.
	
	• Date and time stamp
	
	• Progress bar
	
	An expanded list shows the task's step name and status.
	
	Click the circular icon to refresh the content and fetch recent activity. The page refreshes automatically every 2 minutes.

Recovery list	Displays progress of all recovery-related jobs (for example, migration, recovery, test recovery, re-protect) including the following details:
	
	• ID
	
	• Description
	
	• Task status:
	
	   • **In Progress**
	
	   • **Success**
	
	   • **Failed**
	
	• Date and time stamp
	
	• Progress bar
	
	An expanded list shows the task's step name and status.
	
	Click the circular icon to refresh the content and fetch recent activity. The page refreshes automatically every 2 minutes.

Expand All / Collapse All button	Toggles the view of the job list to display top-level task information or task details. You can also expand and collapse individual tasks.

The following table specifies which Snapshot operations create an HX Task in the Activity Page.

Table 1: Snapshot Operations that create an HX Task in the Activity Page

Operation	HX Task Creation in Activity Page
Ready Clone from HX plugin	No HX task created.
Ready Clone from HX Connect	HX task added to the Activity page.
Scheduled Snapshot task creation from HX Plugin	No HX task created.
Scheduled Snapshot task creation from HX Connect	HX task added to the Activity page.
Snapshot creation from Schedule Snapshot	HX task added to the Activity page.
Snapshot now from HX Plugin	No HX task created.
Snapshot now from HX Connect	HX task added to the Activity page.

System Information Overview Page

Displays HX storage cluster system-related information, including node and disk data, and provides access to HXDP Maintenance Mode.

HX Storage Cluster Configuration Data

Displays the basic configuration information for this HX storage cluster.

UI Element	Essential Information
HX storage cluster field	Name of the storage cluster.
Cluster License Status section	Displays the **Register Now** link when you log into the HX storage cluster for the first time or till the HX storage cluster license is registered:
	Register Now link—To register a cluster license, click this link and provide product instance registration token in the **Smart Software Licensing Product Registration** screen. For more information on how to get a product instance registration token, refer the **Registering a Cluster with Smart Licensing** section in the Cisco HyperFlex Systems Installation Guide for VMware ESXi.
	Note To register a cluster license, you can also choose **Register Now** from the **Actions** drop-down field.

UI Element	Essential Information

License section	• **License Type**—Displays Evaluation, Edge, Standard, or Enterprise as the HX storage cluster license type.
	
	• **License Status**—Displays one of the following as the HX storage cluster license status:
	
	Beginning with HXDP Release 5.0(2a), HX Connect users with expired or insufficient licenses will be unable to access certain features or have limited feature functionality, for more information see the License Compliance and Feature Functionality
	
	    • In compliance
	
	    • License expires in \<n\> days. Cluster not registered - Register Now. (This status appears only for Evaluation type license)
	
	    • License expired. Cluster not registered - Register Now. (This status appears only for Evaluation type license)
	
	    • Out of compliance - Insufficient license
	
	    • Authentication expired—This status appears when HX is unable to communicate with Cisco Smart Software Manager or Smart Software Manager satellite for more than 90 days.
	
	Note To refresh license certificate or renew license authorization, choose the respective options from the **Actions** drop-down field.

HX storage cluster status field	Provides functional status of the HX storage cluster. • **Online**—Cluster is ready. • **Offline**—Cluster is not ready. • **Read Only**—Cluster is out of space. • **Unknown**—Transitional state while the cluster is coming online.
vCenter link	Secure URL to the VMware vSphere associated with this HX storage cluster. Click the link to remotely access the vSphere Web Client .
Hypervisor field	Hypervisor version installed on this HX storage cluster.
HXDP Version field	Installer package version installed on this HX storage cluster.
Data Replication Factor field	Number of the redundant data replicas stored on this HX storage cluster.
Uptime field	Length of time this HX storage cluster has been online.
Total Capacity field	Overall storage size of this cluster.
Available Capacity field	Amount of free storage in this cluster.
DNS Server(s)	IP address for the DNS server(s) for this HX storage cluster.

UI Element	Essential Information
NTP Server(s)	IP address for the NTP server(s) for this HX storage cluster.

Controller VM Access

Use **Actions** to access the controller VM using SSH as an administrator and perform actions such as **Enable Controller Access over SSH**, **Disable Controller Access over SSH** or register your license.

✎

Note   Actions to enable or disable SSH can only be performed by **domain** users, and not local users. Domain users are users in VC (ESXi).

UI Element	Essential Information
Disable Controller Access over SSH	Secure Shell (SSH) is disabled by default.
Register Now	Register your license.
Re-register vCenter	Re-register your license via vCenter
Check Secure Boot Status	Verify your Secure Boot Status

Disk View Options

Customize your Disk View display. Use the check box list to select and deselect the fields that appear in the Node Data section.

Disk View Legend

To display the Disk Legend icons and descriptions, click on **Disk View Legend**.

Node Data

Displays data about individual nodes in this HX storage cluster. To see this information in tabular format, go to the **Nodes** page.

UI Element	Essential Information
Node	Name of a node on this cluster.
Model	Physical hardware model number of this node.
Disks	Number of caching versus persistent disks in this node.
Node status	• **Online** • **Offline** • **In Maintenance** • **Healthy** • **Warning**

UI Element	Essential Information
HXDP Version	HyperFlex Data Platform version installed on this cluster.
Type	• **Hyperconverged** • **Compute**
Hypervisor Status	• **Online** • **Offline** • **In Maintenance** • **In Progress**
Hypervisor Address	IP address for the management network to this HX storage cluster.
Disk Overview	Graphic representation of the number of disks in use for each node, the usage type and number of empty slots. **Note** A disk outline with a red icon indicates a disk that is not recognized and requires a Catalog Upgrade.

For nodes with disks, you can place your cursor over a disk to view an interactive display of information including the following.

Disks

UI Element	Essential Information
Slot Number	Location of the drive, for example Slot Number 2.
Type of Disk	• System • Cache • Persistent
Disk State	• **Claimed** • **Available** • **Ignored** • **Blocked** • **Ok to Remove** • **Unknown**
Locator LED	Activates a physical light on the host to help locate a disk; options are **On** and **Off**.
Capacity	Total disk size.

UI Element	Essential Information
Used / Total Capacity (Persistent Disks only)	Amount of the disk used versus the total disk size.
Serial Number	Physical serial number of this disk.
Storage Usage (Persistent Disks only)	Percentage of disk storage used.
Version	Version of the disk drive.
Disk Drive Interface	The disk drive interface type, for example SAS or SATA.

Nodes Page

Displays data about all of the nodes in this HX storage cluster in a table. Each column can be used to sort the data.

UI Element	Essential Information
Enter HXDP Maintenance Mode button	Select a node to access this button. Opens the **Confirm HXDP Maintenance Mode** dialog box.
Exit HXDP Maintenance Mode button	Select a node to access this button. After you complete any maintenance tasks, you must manually exit HXDP Maintenance Mode.
Node column	Name of a node in this HX storage cluster.
Hypervisor Address column	IP address for the management network of the Node referred in the Node column.
Hypervisor Status column	• **Online**—Node is available. • **Offline**—Node is not available. • **In Maintenance**—The running (and powered off) node is disconnected from the host. • **In Progress**—a backup job is in progress.
Controller Address column	IP address for the HX storage controller VM of the Node referred in the Node column.
Controller Status column	• **Online**—The connection between the VM and the disk is available. • **Offline**—The connection between the VM and the disk is not available. • **In Maintenance**—the connection between the VM and the disk is powered off from the host.

UI Element	Essential Information
Model column	Physical hardware model number of this node.
Version column	HyperFlex Data Platform installer package version installed on this node.
Disks column	Number of disks in the node. Click the number to open the **Disks** page filtered by the selected node name.

Disks Page

Displays data about all of the disks in this HX storage cluster in a 7-column table. Each column can be used to sort the data.

UI Element	Essential Information
Node column	Name of the node where the disk resides.
Slot column	Location of the SED drive. This identifies the drive for maintenance procedures.
Capacity column	Total disk size.

UI Element	Essential Information	
Status column	• **Claimed**—State when a disk is recognized and in use. • **Available**—Initial state for a newly added, data-at-rest capable disk. Also, a transitional state when disks move into one of the other states. • **Ignored**—State when a disk is not being consumed by the cluster; for example, the HX controller VM system disk, a disk with other data (valid file system partitions), or a disk where the IO is failing. • **Blocked**—State when a disk is not being consumed by the cluster due to either a software error or an IO error. This could be a transitional state while the cluster attempts to repair the disk, if the disk is still available, before the state transitions to **Repairing**. • **Ok To Remove**—State when an SED disk was securely erased using the **Secure Erase** option and can safely be removed. • **Repairing**—State when a blocked disk is currently being repaired. • **To Be Removed**—State when a disk is scheduled for RMA.	The following states can be ignored: • **Invalid** • **Normal** • **Removed**—State when an SED disk is removed after using the **Secure Erase** option. • **Time out** • **Unknown**
Encrypted column	• **Enabled**—Encryption is configured for this data-at-rest-capable disk. • **Disabled**—Encryption is not configured for this data-at-rest-capable disk. This occurs when a new disk is present, but the Key has not yet been applied. • **Locked** • **Unknown**	
Type column	• **Unknown** • **Rotational**—Hybrid drive • **Solid State**—SSD drive	

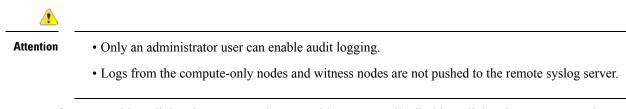| UI Element	Essential Information
Usage column	• **Unknown** • **Cache** • **Persistent**
Turn On Locator LED and **Turn Off Locator LED** radio buttons	Select a disk to access the radio buttons. Activates or deactivates a physical light, or beacon, on the host to help locate the disk.
(Optional) **Secure erase** button	This button in visible only if your HX storage cluster is encrypted using local-key encryption. Select a disk to access the button. Enter the encryption key in use on the cluster, click **Secure erase**, and then click **Yes, erase this disk** to securely erase the local encryption key.

Audit Logging with HX Connect

Audit logging implies storing all audit logs to a remote syslog server. Currently, each controller VM stores audit logs, but these logs are not stored indefinitely. The logs are overwritten based on the retention policy set for the controller VM. By configuring a remote syslog server to store audit logs, you can ensure that the logs are retained for a longer period of time.

Following are the audit logs that you can export to the remote syslog server:

- REST-related logs

    - `/var/log/springpath/audit-rest.log`

    - `/var/log/springpath/hxmanager.log`

    - `/var/log/springpath/hx_device_connector.log`

    - `/var/log/shell.log`

    - `/var/log/springpath/stSSOMgr.log`

    - `/var/log/springpath/hxcli.log`

- `/var/log/nginx/ssl-access.log`

After you enable audit logging, these logs are exported to the remote syslog server. If the logs from the controller VM are not pushed to the remote sylog server, or if the remote syslog server is not reachable, an alarm is generated in the HX-Connect user interface. However, HX Connect does not monitor the disk space available on the remote syslog server. The HX Connect user interface will not display an alarm if the disk on the remote syslog server is full.

⚠️

Attention • Only an administrator user can enable audit logging.

• Logs from the compute-only nodes and witness nodes are not pushed to the remote syslog server.

After you enable audit logging, you can choose to either temporarily disable audit logging, or you can choose to delete the audit logging server configuration details.

Enabling Audit Logging

Before you begin

• Configure the remote syslog server. You must have the server details such as the server IP, the port number and certificate files to enable audit logging in HX-Connect.

• To configure an encrypted connection between the controller VM and the remote syslog server, you must generate a self-signed certificate or a CA-signed certificate and a private key for the syslog client in the controller VM.

• Configure the remote syslog server to categorize different types of logs into respective files.

Step 1 Choose **Settings** > **Audit Log Export Settings**.

Step 2 Check the **Enable audit log export to an external syslog server** check box.

Step 3 Complete the following details:

UI Element	Essential Information
Syslog Server	Enter the IP address of the syslog server.
Port	Enter the port number for the syslog server.
Connection Type drop-down list	Choose **TLS** or **TCP** as the connection type. The default and recommended value is TLS. The TLS connection type is for encrypted transport over TLS. The TCP connection type is for unencrypted transport over TCP.
Client Certificate	Click **Choose** to search and locate a certificate file that must be stored on the controller VM. This certificate creates a TLS connection between the controller VM and the remote syslog server. A TLS connection ensures that the log files are encrypted. You must upload either a user-generated self-signed certificate or a CA-signed certificate.
Private Key	Click **Choose** to search and locate a generated private key file to be stored on the controller VM. This key creates a TLS connection between the controller VM and the remote syslog server. Choosing a certificate and private key for the syslog server ensures that the log files are encrypted. The certificate for the syslog server can either be a CA certificate or a self-signed certificate.

UI Element	Essential Information
Are you using a self-signed certificate?	Check this check box if the syslog server uses a self-signed certificate. Click **Choose** to search and locate the self-signed certificate for the syslog server.

Step 4   Click **OK**.

Configuring the Remote Syslog Server

Prior to enabling audit logging, you must create a configuration file on the remote syslog server to categorize different log files into separate files. You could create a file titled `hx-audit.conf` in the `/etc/syslog-ng/conf.d` directory.

Following is a sample of the configuration file to establish an encrypted connection with the syslog server:

```
## Audit Logging Configuration ###
   source demo_tls_src {
           tcp(ip(0.0.0.0) port(6515)
               tls(
                   key-file("/etc/syslog-ng/CA/serverkey.pem")
                   cert-file("/etc/syslog-ng/CA/servercert.pem")
                   peer-verify(optional-untrusted)
               )
           ); };


   filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
   filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
   filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
   filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
   filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
   filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
   filter f_hxcli { match("hx-cli" value("MSGHDR")); };

   destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
   destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
   destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
   destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
   destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
   destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
   destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

  log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest); flags(final);
 };
   log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
   log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
   log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access); flags(final);
 };
   log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager); flags(final);
 };
   log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
   log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };


########################
```

Following is a sample of the configuration file to establish a TCP connection with the remote syslog server:

```
#######################
## Audit Logging Configuration ###
    source demo_tls_src {
            tcp(ip(0.0.0.0) port(6515)
            ); };

    filter f_audit_rest { match("hx-audit-rest" value("MSGHDR")); };
    filter f_device_conn { match("hx-device-connector" value("MSGHDR")); };
    filter f_stssomgr { match("hx-stSSOMgr" value("MSGHDR")); };
    filter f_ssl_access { match("hx-ssl-access" value("MSGHDR")); };
    filter f_hxmanager { match("hx-manager" value("MSGHDR")); };
    filter f_hx_shell { match("hx-shell" value("MSGHDR")); };
    filter f_hxcli { match("hx-cli" value("MSGHDR")); };

    destination d_audit_rest { file("/var/log/syslog-ng/audit_rest.log"); };
    destination d_device_conn { file("/var/log/syslog-ng/hx_device_connector.log"); };
    destination d_stssomgr { file("/var/log/syslog-ng/stSSOMgr.log"); };
    destination d_ssl_access { file("/var/log/syslog-ng/ssl_access.log"); };
    destination d_hxmanager { file("/var/log/syslog-ng/hxmanager.log"); };
    destination d_hx_shell { file("/var/log/syslog-ng/shell.log"); };
    destination d_hxcli { file("/var/log/syslog-ng/hxcli.log"); };

  log { source(demo_tls_src); filter(f_audit_rest); destination(d_audit_rest); flags(final);
 };
    log { source(demo_tls_src); filter(f_device_conn); destination(d_device_conn);
flags(final); };
    log { source(demo_tls_src); filter(f_stssomgr); destination(d_stssomgr); flags(final);
 };
    log { source(demo_tls_src); filter(f_ssl_access); destination(d_ssl_access); flags(final);
 };
    log { source(demo_tls_src); filter(f_hxmanager); destination(d_hxmanager); flags(final);
 };
    log { source(demo_tls_src); filter(f_hx_shell); destination(d_hx_shell); flags(final);
 };
    log { source(demo_tls_src); filter(f_hxcli); destination(d_hxcli); flags(final); };

#######################
```

Disabling Audit Logging

You can choose to temporarily disable audit logging. By doing so, the remote syslog server details such as the server IP and the port, that you previously configured are retained in the system. You need not enter the server details again when you re-enable audit logging at a later time. You will only need to upload the certificate and private key files to enable audit logging.

Step 1   Choose **Settings** > **Audit Log Export Settings**.

Step 2   Clear the **Enable audit log export to an external syslog server** check box.

Step 3   Click **OK**.

Audit logging is disabled.

Deleting Audit Logging Server Configuration

As an administrator, you can delete the remote syslog server configuration details from the system. When you do so, the system does not push server logs to the remote syslog server. To enable audit logging, you will have to provide the server details again.

Step 1 Choose **Settings** > **Audit Log Export Settings**.

Step 2 Click **Delete**.

Step 3 In the **Confirm Delete** dialog box, click **Delete**.

The remote syslog server details are deleted from the system.